UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,686	01/24/2002	Niels Rump	SCHO0093	3745

7590 01/03/2005	EXAMINER
GLENN PATENT GROUP	HENNING, MATTHEW T
3475 Edison Way	

ART UNIT	PAPER NUMBER
2131	

Suite L
Menlo Park, CA 94025

DATE MAILED: 01/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- Th MAILING DATE of this communication appears on the cover sh et with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 September 2001_.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-31_ is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-31_ is/are rejected.

7)☒ Claim(s) _11-13,19 and 20_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _24 January 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☒ All　b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _12/17/01 et at._.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152) .
6) ☐ Other: _____.

This action is in response to the communication filed on 09/29/2000.

DETAILED ACTION

1.   Claims 1-31 have been examined.

Title

2.   The title of the invention is acceptable.

Priority

3.   The application is a 371 of PCT/EP99/09981, dated 12/15/1999, and claiming priority to

Germany application 19906450.4, filed February 16, 1999.

4.   The effective filing date for the subject matter defined in the pending claims in this

application is February 16, 1999.

Information Disclosure Statement

5.   The information disclosure statements (IDS) submitted on 12/17/2001, 03/18/2002, and

09/23/2004 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is

considering the information disclosure statement.

Drawings

6.   The drawings filed on 01/24/2002 are acceptable for examination proceedings.

Specification

7.   Applicant is reminded of the proper language and format for an abstract of the disclosure.

*The abstract should be in narrative form and generally limited to a single paragraph on
a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed
150 words in length since the space provided for the abstract on the computer tape used by the
printer is limited. The form and legal phraseology often used in patent claims, such as "means"
and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist
readers in deciding whether there is a need for consulting the full patent text for details.*

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

8.   The abstract of the disclosure is objected to because

Lines 1-3: "Method and device…payload data stream" must be removed, as it is not a

proper heading for the Abstract of the Disclosure.

Correction is required. See MPEP § 608.01(b).

Claim Objections

9.   Claims 11-13, and 19-20 are objected to for failing to conform to standard claim

numbering.

The applicant is reminded that a series of singular dependent claims is permissible in

which a dependent claim refers to a preceding claim which, in turn, refers to another preceding

claim.

A claim which depends from a dependent claim should not be separated by any claim

which does not also depend from said dependent claim. It should be kept in mind that a

dependent claim may refer to any preceding independent claim. In general, applicant's sequence

will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 112

10.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11.   Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

12.   Claim 1 recites the limitation "linking said information containing said payload data key" in Lines 17-18. There is insufficient antecedent basis for this limitation in the claim. For the purposes of searching prior art, the examiner will assume that the claim was meant to read "linking said information and said payload data key" as is consistent with claim 28.

13.   Claim 7 recites the limitation "said algorithm being used in said step of processing" in lines 4-5. This is inconsistent with claim 1, from which claim 7 depends, in which the only algorithm mentioned is a "payload data encryption algorithm" used in the step of encrypting, and not in the step of processing. Therefore, one of ordinary skill in the art would be unable to determine the scope of this claim, because the ordinary person of skill in the art would be unable to determine whether "said algorithm" referred to the encryption algorithm or a different undisclosed algorithm.

14.   Claim 8 recites the limitation "said data" in line 3. The ordinary person skilled in the art would be unable to determine whether "said data" was meant to refer to the license data, or the payload data.

15.   Claim 11 recites the limitation "said license data" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim. The examiner will assume for purposes of searching art that claim 11 was meant to depend on claim 8, which is consistent with 9-10, and 12-13.

16.   Any claim not specifically mentioned is rejected by virtue of its dependency to an above rejected claim.

Claim Rejections - 35 USC § 102

17.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(e) the invention was described in (1) an application for patent, published under section
> 122(b), by another filed in the United States before the invention by the applicant for
> patent or (2) a patent granted on an application for patent by another filed in the United
> States before the invention by the applicant for patent, except that an international
> application filed under the treaty defined in section 351(a) shall have the effects for
> purposes of this subsection of an application filed in the United States only if the
> international application designated the United States and was published under Article
> 21(2) of such treaty in the English language.*

18.   Claims 1-7, 14, 16-17, 19, 23, 25-28, and 30 are rejected under 35 U.S.C. 102(e) as being

anticipated by Van Oorschot et al. (US Patent Number 5,850,443) hereinafter referred to as Van

Oorschot.

19.   Regarding claim 1, Van Oorschot disclosed a method for producing a payload data

stream comprising a header and a payload data block containing encrypted payload data (See

Van Oorschot Fig. 3 X-fields, header fields, and encrypted message field), comprising the

following steps: generating a payload data key for a payload data encryption algorithm for

encrypting payload data (See Van Oorschot Col. 6 Lines 41-43 and Fig. 3 "Create low trust

symmetric key"); encrypting payload data using said payload data key and said payload data

encryption algorithm to obtain an encrypted section of said payload data block of said payload

data stream (See Van Oorschot Col. 6 Lines 42-43 and Fig. 3 "Symmetric encryption" and

"encrypted message"); processing a part said payload data stream (See Van Oorschot Fig. 3 "X-

fields") to deduce information marking said part of said payload data stream (See Van Oorschot

Col. 6 Lines 49-55); linking said information containing said payload data key by means of an

invertible logic linkage to obtain a basic value (See Van Oorschot Col. 6 Lines 56-60);

encrypting said basic value using a key of two keys being different from each other by an

asymmetrical encryption method, said two different keys being the public and the private keys

respectively for said asymmetrical encryption method, to obtain an output value being an

encrypted version of said payload data key (See Van Oorschot Col. 6 Line 60 – Col. 7 Line 7);

and entering said output value into said header of said payload data stream (See Van Oorschot

Col. 6 Line 65 – Col. 7 Line 7 and Fig. 3 "A's header field" and "B's header field").

20.   Regarding claim 2, Van Oorschot disclosed that said payload data encryption algorithm is

a symmetrical encryption algorithm (See Van Oorschot Fig. 3 "symmetric encryption").

21.   Regarding claim 3, Van Oorschot disclosed that said invertible logic linkage is self-

inverting and includes an XOR- linkage (See Van Oorschot Col. 6 Lines 56-60).

22.   Regarding claim 4, Van Oorschot disclosed that one key of said two keys being different

from each other is the private key of a producer of said payload data stream or the public key of a

consumer of said payload data stream (See Van Oorschot Fig. 3 B's high trust public key).

23.   Regarding claim 5, Van Oorschot disclosed that said part of said payload data stream

being processed to deduce said information includes at least a part of said header (See Van

Oorschot Fig. 3 "X-Field" and Col. 6 Lines 49-55).

24.   Regarding claim 6, Van Oorschot disclosed that said step of processing comprises

forming a hash sum (See Van Oorschot Col. 6 Lines 49-55).

25.   Regarding claim 7, Van Oorschot disclosed further comprising the following step:

identifying said algorithm being used in said step of processing by an entry into said header (See

Van Oorschot Abstract Lines 14-16).

26.   Regarding claim 14, Van Oorschot disclosed that said step of processing further

comprises the following sub-step: setting said entry for said output value in said header to a

defined value and processing said entire header, including said entry set to a defined value (See

Van Oorschot Fig. 3 "X-Field" and Col. 6 Lines 49-55).

27.   Regarding Claim 16, Van Oorschot disclosed the following step: identifying said payload

data encryption algorithm by an entry into said header of said payload data stream (See Van

Oorschot Abstract Lines 14-16).

28.   Regarding claim 17, Van Oorschot disclosed Method for decrypting an encrypted

payload data stream comprising a header and a payload data block containing encrypted payload

data, said header comprising an output value having been generated by an encryption of a basic

value by an asymmetrical encryption method using a key of two different keys including a

private and a public key, said basic value representing a linkage of a payload data key, with

which said encrypted payload data is encrypted using a payload data encryption algorithm, and

information deduced by a certain processing, said information marking a certain part of said

payload data stream unambiguously (See rejection of claim 1 above), said method comprising

the following steps: obtaining said output value from said header (See Van Oorschot Fig. 4 "B's

Header Field" and Col. 4 Lines 51-52); decrypting said output value using the other key of said

asymmetrical encryption method to obtain said basic value (See Van Oorschot Fig. 4 "private

key decryption" and ""B's high trust private key" and Col. 4 Lines 53-54); processing a part of

said payload data stream using the processing method used for encrypting to deduce information

marking said part, said part corresponding to said certain part when encrypting (See Van

Oorschot Fig. 4 "X-fields"); linking said information and said basic value using the .

corresponding linkage as it has been used when encrypting to obtain said payload data key (See Van Oorschot Fig. 4 "Unlevelling" and "X-fields" and Col. 4 Lines 54-56); and decrypting said block containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting (See Van Oorschot Fig. 4 "symmetric decryption" and "message").

29.   Regarding claim 19, Van Oorschot disclosed that said part being processed to deduce said information is said header (See Van Oorschot Fig. 4 "X-Fields").

30.   Regarding claim 23, Van Oorschot disclosed that one key having been used when encrypting is the public key of said asymmetrical encryption method, while the other key having been used when decrypting is the private key of said asymmetrical encryption method (See Van Oorschot Fig. 3 "B's high trust public key" and Fig 4 "B's high trust private key").

31.   Regarding claim 24, Van Oorschot disclosed that said step of processing includes forming a hash sum (See Van Oorschot Col. 6 Lines 49-55 and Fig. 4 "Unlevelling").

32.   Regarding claim 25, Van Oorschot disclosed that a part of said header having been set to a defined value for said step of processing when encrypting is set to the same defined value for said step of processing when decrypting (See Van Oorschot Fig. 3 "X-fields" and Fig. 4 "X-fields" wherein they must be the same defined value because they were both set by the sender upon sending).

33.   Regarding claim 26, Van Oorschot disclosed that said part of said header being set to a defined value includes said entry for said output value of said header (See Van Oorschot Fig. 3 "B's header field" and Fig. 4 "B's header field" wherein they must be the same defined value because they were both set by the sender upon sending).

34.	Regarding claim 27, Van Oorschot disclosed that said step of linking comprises using an

XOR-linkage (See Van Oorschot Col. 6 Lines 56-60 and Col. 4 Lines 54-56 and Fig. 4

"Unlevelling".

35.	Claim 28 is rejected for the same reasons as claim 1 above and further because Van

Oorschot disclosed both the method and apparatus (See Van Oorschot Claims).

36.	Claim 30 is rejected for the same reasons as claim 17 above and further because Van

Oorschot disclosed both the method and apparatus (See Van Oorschot Claims).

Claim Rejections - 35 USC § 103

37.	The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a whole
> would have been obvious at the time the invention was made to a person having ordinary
> skill in the art to which said subject matter pertains. Patentability shall not be negatived
> by the manner in which the invention was made.*

38.	Claims 8, 11-12, 18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Van Oorschot as applied to claims 1 and 17 above, and further in view of Matyas et al. (US

Patent Number 5,200,999) hereinafter referred to as Matyas.

Van Oorschot disclosed a system for sending a message from a sender to a receiver in

which the message was encrypted using a key, the key was encrypted, and then the key was sent

to the receiver with the encrypted message (See Van Oorschot Abstract and Fig. 3). Van

Oorschot further disclosed decrypting the key, and using the key to decrypt the message at the

receiver (See Van Oorschot Abstract and Fig. 4). However, Van Oorschot failed to disclose

sending license data along with the key and message.

Matyas teaches that when sending a key, in order to authenticate the use of the key, and
the validity of the key, certain data (License data) should be placed in the header along with the
key. This data includes key type, key usage data (for history purposes), algorithm identifier,
algorithm-specific data, key start date/time, key expiration data/time, device identifier, user
identifier, key identifier, logical device identifier, and user-defined data (See Matyas Col. 13
Line 66 – Col. 14 Lines 60). Matyas further teaches that this information should be verified
prior to use of the key (See Matyas Col. 100).

It would have been obvious to the ordinary person skilled in the art at the time of
invention to employ the teachings of Matyas in the key and message sending system and method
of Van Oorschot by placing the license information, taught by Matyas, in the header of the
message and checking this information prior to allowing the key and message to be decrypted.
This would have been obvious because the ordinary person skilled in the art would have been
motivated to protect the interests of the sender of the message and to ensure the security of the
message.

39.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of

Van Oorschot and Matyas as applied to claim 8 above, and further in view of Klemba et al. (US

Patent Number 5,710,814) hereinafter referred to as Klemba.

Van Oorschot and Matyas disclosed sending license data for controlling the usage of a

key and message, including usage history (See rejection of claim 8 above), but failed to disclose

the data including how often the message could be decrypted.

Klemba teaches that license data can be used to control the number of uses of a

cryptographic function (See Klemba Col. 14 Lines 14-19).

It would have been obvious to the ordinary person skilled in the art at the time of

invention to employ the teachings of Klemba in the messaging system and method of Van

Oorschot and Matyas by using the license information to limit the number of times the message

could be decrypted. This would have been obvious because the ordinary person skilled in the art

would have been motivated to protect the interests of the sender of the message as well as to

protect the message against compromise.

40.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination

of Van Oorschot and Matyas as applied to claim 8 above, and further in view of Edenson et al.

(Us Patent Number 6,198,875) hereinafter referred to as Edenson.

Van Oorschot and Matyas disclosed sending license data for controlling the usage of a

key and message, including usage history (See rejection of claim 8 above), but failed to disclose

the data including how often the message could be copied and how often it had already been

copied.

Edenson teaches that license information can include how many copies of licensed data

can be made (See Edenson Col. 4 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of

invention to employ the teachings of Edenson in the messaging system of Van Oorschot and

Matyas by including information regarding the number of allowed copies of the message that are

permitted. This would have been obvious because the ordinary person skilled in the art would

have been motivated to protect the interests of the message sender, and to protect the message

itself from unauthorized distribution. Further, it would have been necessary to also keep track of

the number of copies already made in order to enforce the copy limit.

41.   Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination

of Van Oorschot and Matyas as applied to claim 8 above, and further in view of Schneier

("Applied Cryptography Second Edition").

Van Oorschot and Matyas disclosed sending license data for controlling the usage of a key and message, including usage history (See rejection of claim 8 above), but failed to disclose including the license in the hash function.

Schneier teaches that hashes are used to authenticate the data being hashed upon receipt of the data in order to detect any unauthorized changes to the data (See Schneier Pages 30-31 Section 2.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the messaging system of Van Oorschot and Matyas by hashing the License data along with the X-fields. This would have been obvious because the ordinary person skilled in the art would have bee motivated to protect against undetected changes to the license data sent with the message.

42.   Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot as applied to claim 1 above, and further in view of Roediger (US Patent Number 4,899,333).

Van Oorschot disclosed sending a message from a sender to a receiver, including a header and a hash of the header (See Van Oorschot Col. 6), but Van Oorschot failed to disclose including a sender identifier and a receiver identifier in the header, or in the hash.

Roediger teaches that packet headers contain and source address (sender identifier) and a destination address (recipient identifier) and that a checksum should include these fields in order to ensure that the fields are not corrupted (See Roediger Col. 37 Lines 53-63).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Roediger in the messaging system of Van Oorschot by including source and destination addresses in the header and including these in the hash. This

would have been obvious because the ordinary person skilled in the art would have been

motivated to provide means for routing the message from the sender to the receiver and allowing

the receiver to verify that it was the intended receiver of the message.

43.   Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot as

applied to claim 17 above, and further in view of Schneier.

        Van Oorschot disclosed using a public key of the receiver for encryption (See rejection of

claim 23 above) but failed to disclose using a private key of an asymmetrical key pair for

encryption.

        Schneier teaches that by encrypting data using a senders private key, the receiver can use

the senders public key to authenticate the sender of the data (See Schneier Pages 53-54).

        It would have been obvious to employ the teachings of Schneier in the messaging system

of Van Oorschot by encrypting the leveled key with the private key of the sender and decrypting

it with the public key of the sender. This would have been obvious because the ordinary person

skilled in the art would have been motivated to provide sender authentication at the receiver.

44.   Claims 29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van

Oorschot as applied to claims 28 and 30 above, and further in view of Kane et al. (US Patent

Number 5,315,635) hereinafter referred to as Kane.

        Van Oorschot disclosed sending messages from a sender to a receiver (See Van Oorschot

Abstract), but failed to disclose the sending being from a personal computer to a personal

computer.

        Kane teaches that messages can be sent between personal computers (See Kane Col. 1

Lines 45-51).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kane in the messaging system of Van Oorschot by sending the encrypted messages from a sending personal computer to receiving personal computer. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect messages sent between two personal computers.

Conclusion

45.   Claims 1-31 have been rejected.

46.   Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (571) 272-3790. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131

12/21/04

EMMANUEL L. MOISE
PRIMARY EXAMINER